

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date  
14 July 2005 (14.07.2005)

PCT

(10) International Publication Number  
WO 2005/064973 A1

(51) International Patent Classification<sup>7</sup>: H04Q 7/38, 7/32, H04L 29/06

(21) International Application Number: PCT/EP2003/051101

(22) International Filing Date: 24 December 2003 (24.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): ARKKO, Jari [FI/FI]; Kauppalantie 25 A 7, 02700 Kauniainen (FI). NIKANDER, Pekka [FI/FI]; OY LM Ericsson, Hirsalantie 1, 02420 Jorvas (FI).

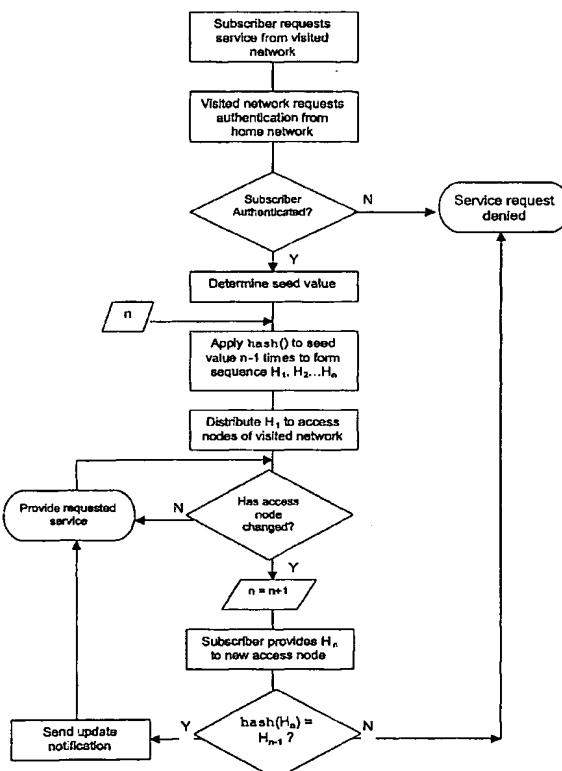
(74) Agents: LIND, Robert et al.; Marks & Clark, 4220 Nash Court, Oxford Business Park South, Oxford, 48 OX4 2RU (GB).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: AUTHENTICATION IN A COMMUNICATION NETWORK



(57) Abstract: A method of authenticating a mobile node to a communication system is provided, the communication system comprising a plurality of access nodes, the method comprising the steps of (a) generating a numerical chain comprising a series of values using a oneway coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; (b) sending a value from the first numerical chain from the mobile node to an access node to which the mobile node wishes to attach; and (c) using the sent value at the access node to authenticate the mobile node.

WO 2005/064973 A1



**Published:**

— *with international search report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*